Notice of Allowability	Application No.	Applicant(s)	
	10/058,689	BRUTON ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the RCE received 24 October 2006*.

2. ☒ The allowed claim(s) is/are *1,3-15,22,24-27,32,34-40 and 45-58*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

EXAMINER'S AMENDMENT

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 20 September 2006 has been entered.

2. By the above submission, Claims 1, 3, 9-11, 15, 22, 24, 26, 27, 32, 34, 35, 37, 40, 45, and 54-56 have been amended. No claims have been added or canceled. Claims 1, 3-15, 22, 24-27, 32, 34-40, and 45-58 are currently pending in the present application.

Examiner's Amendment

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Marcia Doubet on 08 December 2006.

The application has been amended as follows:

IN THE CLAIMS:

Please **REPLACE Claims 22 and 32** with the following amended claims:

22. A system for improving intrusion detection in a computing network, comprising:

a definition of a plurality of intrusion suspicion levels for use when performing intrusion detection processing on inbound communications destined for a computing device on the computing network;

for each of a plurality of potential intrusion events, a definition of a set of at least one condition, wherein the set describes occurrence of the potential intrusion event;

means for associating one of the defined intrusion suspicion levels with each of the defined sets, wherein the associated intrusion suspicion level indicates how suspicious is an inbound communication matching each condition in the set;

a definition of a plurality of sensitivity levels for filtering the inbound communications as potential intrusion events when performing the intrusion detection processing, each of the defined sensitivity levels usable for a different level of filtering of the inbound communications; and

means for performing the intrusion detection processing for a particular inbound communication received for the computing device, further comprising:

~~means for determining whether each condition in any of the sets is matched for the particular inbound communication; and~~

~~if so,~~ means for filtering the particular inbound communication, if each condition in any of the sets is matched for the particular inbound communication, by using a currently-applicable one of the defined sensitivity levels, in concert with the intrusion suspicion level associated with the set for which each condition is matched, to determine if the particular inbound communication destined for the computing device should be treated as an intrusion event.

32. A computer program product for improving intrusion detection in a computing network, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable code defining a plurality of intrusion suspicion levels for use when performing intrusion detection processing on inbound communications destined for a computing device on the computing network;

for each of a plurality of potential intrusion events, computer-readable program code defining a set of at least one condition, wherein the set describes occurrence of the potential intrusion event;

computer-readable program code associating one of the defined intrusion suspicion levels with each of the sets, wherein the associated intrusion suspicion level

indicates how suspicious is an inbound communication matching each condition in the set;

computer-readable program code defining a plurality of sensitivity levels for filtering the inbound communications as potential intrusion events when performing the intrusion detection processing, each of the defined sensitivity levels usable for a different level of filtering of the inbound communications; and

computer-readable program code for performing the intrusion detection processing for a particular inbound communication received for the computing device, further comprising:

~~computer-readable program code for determining whether each condition in any of the sets is matched for the particular inbound communication; and~~

~~if so,~~ computer-readable program code for filtering the particular inbound communication, if each condition in any of the sets is matched for the particular inbound communication, by using a currently-applicable one of the defined sensitivity levels, in concert with the intrusion suspicion level associated with the ~~matched~~ set for which each condition is matched, to determine if the particular inbound communication destined for the computing device should be treated as an intrusion event.

Allowable Subject Matter

4. Claims 1, 3-15, 22, 24-27, 32, 34-40, and 45-58 are allowed.

5. The following is an examiner's statement of reasons for allowance:

Independent Claims 1, 22, and 32 are directed to a method, system, and software implementation of the method for performing intrusion detection on a network, in which sets of conditions are defined for inbound communications, a previously-defined suspicion level is associated with communications matching each condition in a set, and intrusion detection is performed by filtering the communications based on the associated suspicion level and a currently-applicable sensitivity level, which was previously defined to be used for a specific level of filtering. The previously cited prior art, Vaidya, US Patent 6279113, discloses an intrusion detection system in which attack profiles are used to raise the sensitivity to certain actions which are implicitly considered more suspicious based on the profile and other actions that have been performed (see column 7, line 52-column 8, line 39); however, although suspicion and sensitivity levels may be generally implied by Vaidya's disclosure, Vaidya does not explicitly disclose the use of suspicion and sensitivity levels as specifically and explicitly described in the currently amended independent claims. Additionally, Moore et al, US Patent 7114185, discloses a system for scanning files for viruses or other malware, where the scanning may be made more sensitive by reducing a threshold of a scoring of suspicious activities used to identify the malware (see, for example, column 5, lines 40-51); however, while a virus could be considered to be a type of intrusion, Moore only

discloses scanning files already on a system, and does not suggest actively scanning or filtering communications inbound to a computer system in a network as explicitly claimed. Therefore, the claims are patentable over the cited prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Moran, US Patent 7085936, discloses an intrusion detection system that assigns suspicion values to various events.

b. Farley et al, US Patent 7089428, discloses a security system including intrusion detection systems that uses information from several intrusion detection systems to correlate whether a pattern of events is suspicious.

c. Manganaris et al, US Patent Application Publication 2002/0082886, discloses an intrusion detection system that determines the suspicion of various alarms.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad